~~TOP SECRET~~

ARMY SECURITY AGENCY

68/49/TOPSECRET/AS-14

Copy No. 5

From: CSGAS-14

To: AS-95 (for additional routing within AS-90)

~~TOP SECRET~~

~~TOP SECRET~~

DF-169

68/49/~~TOP SECRET~~/AS-14

CRYPTANALYTIC SECTION JAPANESE FOREIGN OFFICE

Attached are translations of Japanese TICOM reports resulting from the investigation of the Japanese Foreign Office. It will be recalled that TICOM teams in Japan were at first instructed to avoid any investigation of the Japanese Foreign Office because of the danger of compromising Allied knowledge of the cryptographic system which was still being used by the Japanese diplomatic representatives then abroad. By November 1945 it became possible to investigate the Japanese Foreign Office and officers from Army Security Agency Pacific interrogated former members of the Japanese Foreign Office Cryptanalytic Section, and in some cases secured from them "homework".

The translations of these interrogations and documents have been made at Army Security Agency and ASA Pacific. Originals of all translations are available at Army Security Agency.

July 1949 — 30 copies; Copy No. 4

Translated at ASA/ Pacific — 49 pages

~~TOP SECRET~~

~~TOP SECRET~~

TABLE OF CONTENTS

~~TOP SECRET~~

~~TOP SECRET~~

ADVANCED GENERAL HEADQUARTERS
UNITED STATES ARMY FORCES, PACIFIC
OFFICE OF THE CHIEF SIGNAL OFFICER
SIGNAL INTELLIGENCE DIVISION

APO 500
11 December 1945

MEMORANDUM:

TO : Major General S. B. Akin

SUBJECT : Foreign Office Cryptanalytic Section

1. Investigations of the Foreign Office Cryptanalytic Section have disclosed little real information to date. Some difficulty is being experienced in rounding up personnel and getting them back into Tokyo. However, we have contacted the head of the organization, Mr. Fukuda, and have learned the following:

a. The organization, founded in 1923, had 14 men of official rank and 16 typist-clerks on its roster at the end of the war.

b. Mr. Fukuda's association with the organization only dates back to December 1943.

c. Cryptanalysis on diplomatic systems used by representatives and offices of the United States, England, China and France was the sole commitment of this organization.

d. Technical liaison was carried out with both army and navy cryptanalytic sections.

2. Arrangements have been made to interview the following:

a. Mr. Kudo, head of the organization prior to Mr. Fukuda assuming that office.

b. Mr. Michida, head of the intercept service and in charge of the main intercept station at Higashi-Kurume Mura, Tokyo.

c. Mr. Fujimi, assistant to Mr. Fukuda, head of the technical group working on U.S. and British systems.

d. Mr. Yoshihara, head of the technical group working on Chinese systems.

3. Further reports will be forthcoming.

H.S.E.

~~TOP SECRET~~

~~TOP SECRET~~

II. SOME TRANSACTIONS WHICH TRANSPIRED WHILE ON DUTY IN THE ANNEX ROOM (SPECIAL SECTION OF THE COMMUNICATION SECTION OF THE FOREIGN OFFICE

TOYOKI FUKUDA
Communications Officer, Foreign Office

I was ordered to report for duty to the Annex Room of the Communication Section in December, 1940. Before this, I attended lectures given by Mr. SUGIYAMA, a special employee of that office, on the fundamentals of code solution.

Mr. HAYATO KUDOO, Communication Officer, was the head of this section at the time of my assignment.

The scope of my assignment was to perform research on all diplomatic codes of countries linked with the German language, but because I had only three assistants and since only one of them had any capabilities for research of this nature, I limited our field to German codes alone.

One of the German codes which we succeeded in reading was the one-volume alphabetically arranged code which had DESAB as an indicator and which contained 100,000 values. We were able to solve about one-third of its total values by April 1945 when Germany collapsed.

In the summer of 1942 we succeeded in reading a part of a coded message which used the DESAB code and additives (YU GEN RANSUU). This was because of the carelessness on the part of some official in the German Embassy in Tokyo when he used the same additives several times in messages dispatched from that office.

In April, 1943 Mr. KUDOO resigned his post and I succeeded him as head of the section. At the time, there were, in addition to myself, the following section chiefs:

Section	No. of Persons in Section
Foreign Office Code Compilation	3
British-United States	6
French	2
Chinese	4
German	4

There were several other persons doing odd jobs.

Since the heads of the above-mentioned sections were under the direct control of the Chief of the Communication Section, the Chief of the Annex

Room (Special Section) as a head had practically no power. Under the circumstances my work was limited to research on German codes and to compilation of and research on Japanese codes. In view of this fact the Army and Navy attached little or no importance to ths research done by the Foreign Office.

With the resignation of some of the personnel in April, 1945 young capable officers were appointed as heads of various sections. As listed in the chart already presented, Mr. SEI HAYAKAWA became the head of the British-United States solution section (JITSUMU) and Mr. ZENKATSU FUJIMI became the head of the research section, but with the change of the war situation more people were called to the colors and it became extremely difficult to recruit qualified personnel. When the United States air raids became fiercer, some of our personnel were killed and others lost their homes and furniture, and, in this way, efficiency gradually dropped off because no one was settled to work. This condition continued until 15 August when the war ended and when the operation of the Special Section ended as of same date.

Yoshi Kato

The codes which we were able to read after I became the head of the Special Section were:

a. French CGX Code: In the spring of 1943 we received the CGX Code and its substitution table (KAEJIHYOO) from the Army but we did not understand how it was used. I assigned my assistant, Mr. MASAJI KOMIYA (he is still missing since the air raids of 9 and 10 March and is now considered killed), to make this research in May of the same year (1943). As a result of his studies, in September 1943 we were able to find out how the substitution table was used and also the fact that the substitution table was for use with another code. Since France had already fallen at this time, the use of this code was of no practical value. I do not clearly recall the name of the code with which the substitution table was used, but I think it was "C-149". I cannot state in detail how the substitution table was used because Mr. KOMIYA, who was in charge, is now dead.

b. We made some progress in our research on the United States strip cipher. As explained to you by Mr. FUJIMI and myself in a separate document, we discovered that we could reconstruct the strips if we could obtain both

cipher and plain texts. In our study of the cipher text alone, however, we discovered many false frequencies and it became extremely difficult to differentiate them from the true ones. This problem was not solved before the end of the war.

c. The codes which we received from the Army were as follows:

Portuguese Diplomatic Code.....Spring 1943

Spanish Diplomatic Code..... (?) 1944

French CGX Code and its Substitution Table.....Spring 1944

Italian Commercial Attache Code.....Spring 1945

Swiss Diplomatic Code.....Summer 1945

Of this group the French and Italian codes were intended for use in the period after the respective countires had fallen, so they were of no value; as to the others, there was little opportunity to make special use of them. Since they are now gone, I cannot give you any detailed explanation regarding them.

Some of the codes which we were able to read before I joined or became the head of the Special Section were: The Chinese and the Thailand diplomatic codes. In regard to the former, I believe Mr. DAIZOO YOSHIHARA has already made an explanation. The latter was a 5-digit code which used a simple additive system. The code book was in one volume and it was in English terms alphabetically arranged. Besides these there were several types of French diplomatic codes and a Swiss International Settlement Code. Since these code books are now destroyed, I cannot go into detail. Both of the above-mentioned codes were obtained from the Army. We gave up our research on the British and the Soviet Union codes becuase their degree of security was high and because we lacked qualified personnel.

I know that there are parts in the above explanation which are not sufficient. These are due to the irregular position the head of the Special Section occupied and also becuase I had to rely on my recollection alone since

all the records of the Special Section were burned before 15 August by the order of the superior. In view of these facts, I request that you understand the situation.

III. FOREIGN OFFICE PRESS INTERCEPT STATION

Interrogators' note: The intercept station located at Tōkyō-To, Kitatama-Gun, Kurumemura-Gun, Kōyama was and is at present concerned only with press and official releases of foreign countries. These were intercepted in both plain language and code in about equal amounts. Only tape recording was practiced, and after being copied by typewriter, the messages were carried to Tokyo once a day by courier.

The average number of messages taken per day was 40 to 60 during wartime, with 100 the maximum. Nineteen operators, divided into three shifts of four people, were on duty at receivers during peak operation. Division of this personnel is as given in the appended translated report.

Of the 10 receivers, only five were in operating condition, and during the war, only four were said to be operated at any one time. This was said to be due to a scarcity of tubes, parts, etc., on which the Army had highest priority. There was evidence at the station of a remarkable scarcity of all accessory materials.

Further difficulty was encountered, according to authorities at the station, in the matter of power supply since the nearby Nakajima aircraft factory often drew power from the local supply to such an extent that facilities at this station became inoperative.

Attached is a translation of a report furnished by Mr. MACHIDA, technical director of the station. Commitments for each set were dictated by Mr. OYE of the Foreign Office, and apparently frequencies within the limits allotted to each set were searched at random for copyable press broadcasts.

12 December 1945

SUBJECT: Report on Foreign Office Signal Station Equipment, etc.

1. Types and number of receivers.

MANUFACTURER	DESIGNATION	NO. OF TUBES	RECORDING GEAR	QUANTITY	REMARKS
Japan Wireless & Telegraph Co.Ltd.	RSA46A	46	Moving coil tape recorder	8 sets	4-6 used during wartime; 3-4 at present.
"	RSA46B	46	Tape recorder	2 sets	Not used due to unsatisfactory results of testing.
"	RSA16A	16	Moving coil tape recorder	1 set	Used for freqency search
"	RSA13A	13	Damaged	2 sets	Not used due to damage

2. Power used.

USE	DAILY CONSUMPTION	REMARKS
(a) Receivers		Supplied during peacetime from civilian power lines, during wartime by military ownership.
(b) Pumps (hydraulic)	Total of 100-300 kw	Consumption high, causing many instances of power drop and failure of receivers to operate.
(c) Lighting and heating (winter)		Failure of current due also to defective power lines.

3. Intercept data.

COUNTRY	STATION CALL SIGN	FREQUENCY (kc)	CONDITION OF RECEPTION	RECEIVER	DAILY AVERAGE NO. OF MSGS.
Chinese National Republic	XTC	9285	Reception of XQH and XOJ good; others often impossible due to jamming by military communications.	#2	6
	XQH	?			
	XTQ	?			
	XOJ	15795			
	XGN	16390			
	XGR	2540			
	XGV	7410			
America	KNK	6875	Reception very good.		
	KJA	10570			
	KWT	13750			
	KWA	7655		#4	15
	KUN	17170			
	KNN	17420			
	KGT5	?			
	KGT7	?			
India	VWX2	18210	Reception good (received only during day time).	#5	20
	VWN3	?			
Turkey	TAG	13090	Reception only during night time. From June to August strong atmospherics prevented reception. December to April best time for reception.	#5	20
	TAF	8045			
Switzerland	HBE	15005	Difficult due to extreme-ly weak reception. April to June maximum receptivity; at other times very poor.	#6	5
	HBC	9000			
	HBR	7900			
	HBS	14945			
England	GLY	11420	Receptivity very poor. Interruptions frequent during night.	#6	3
	GMX	15020			
	GLG	19060			
	GOF	7600			
	GLQ	10930			
AMERICA	KROX	9530	Receptivity very good.	#7	10
		9855			
		17880			
	KROZ	5985			
		9897			
		15100			
	KWE	15430			
	KER	10390			
	KHF4	?			
	KGT3	?			
	KGT6	?			
America	KWQ	13260	Receptivity very poor.	#8	3
	KWD	8990			
	KEJ	9010			

COUNTRY	STATION CALL SIGN	FREQUENCY (kc)	CONDITION OF RECEPTION	RECEIVER	DAILY AVERAGE NO. OF MSGS.
Soviet Russia	RLK RBT	? 8055 11490	Frequent jamming; receptivity poor.	#8	

Notes:

(1) Receivers #1 and #2 were not in use due to breakdown. Nos. 3-8 also often failed due to tube and other parts shortages. On the average four to five sets (six at most) were used during wartime, and were engaged in the reception of press and official dispatches, in about equal quantities.

(2) After the conclusion of the war, three to four sets were used, chiefly for the reception of "broadcast press."

4. Antennae.

TYPE	DIRECTION	NUMBER	OBJECTIVES OF RECEPTION	NOTES
Beam	Europe	2		Not put into operation due to insufficient wire, etc.
Rhombic	America	2	San Francisco, Los Angeles.	
Rhombic	Europe	1	Turkey, Bombay, London, Switzerland, Irkutsk.	
L-type	---	2 (14 lines)	China, Irkutsk, Bombay (Search)	

5. History and Subordination of Station.

(a) Established middle of November, 1941.
(b) Directly subordinate to the Chief, Telegraphic Section of the Foreign Office.

6. Personnel Details.

Deputy Chief, Foreign Office, Technician MACHIDA SEIICHI

"A" squad	-Squad Leader, Foreign Office technician TANAKA	Specialists:	BABA FUDESUKE, SANADA SHOSEI MOGI TSUHEI
"B" squad	-Squad leader, Foreign Office technician IKEDA SEIKICHI	Specialists:	SAKURAI AKIRA MORI YOSHIO OGAWA UKICHI
"C" squad	-Squad leader, ISHI KIYO	Specialists:	HAMAOKA HIKOJI KAWANO TOKICHI ITŌ IPPEI
Administrative		Specialists:	ENTŌ MITSURO FUKUSHIMA HIDEO

NOTES: Persons detailed to the office since end of war.

Technician	MATSUURA ISABURO
Ass't Technician	TAKAHASHI SŌICHI
Specialist	MISU SHIGE

IV. CIRCUMSTANCES SURROUNDING OUR RESEARCH ON AMERICAN STRIP CIPHERS

TOYOKI FUKUDA
Communications Officer, Foreign Office

On 22 August 1943 Colonel NAKANO of the Army sent us the version of the American diplomatic strip cipher used between Vichy and Washington, which had been reconstructed as a result of his studies. Mr. HAYATO KUDOO, then chief of the Communications Section of the Foreign Office, ordered me to carry on similar research along this line.

I studied these strips carefully but was not able to understand how they could be reconstructed from mere research because I lacked sufficient research materials. I shall attempt, however, to explain the process we followed by use of examples and the manner in which the materials on hand (the records of these materials are gone so I cannot say for sure, but I believe they were sent to the Annex Room by the Army before I took up this research) were utilized in our research.

First, we wrote the cipher text below the plain text and looked for frequencies (HAMPUKU). As a result of that study, we discovered that the periods were either 15 or 30. Therefore, we divided the plain and cipher texts into 15-or 30-letter groups, and made each of them into a long separate strip.

Next, we looked for frequencies in order to find out the sequent letter order of each strip used. When the interval (KANKAKU) between letters of both the cipher and plain texts appeared the same, we discovered that the same frequencies also appeared.

EXAMPLE

The Japanese	Three Powers
QST WDAEC...	QSGRP AXQ...

We gathered strips with the same frequency into one group and other strips of similar category into another group and made a study of the sequent letter order of the strips by comparing the various groups.

If you study the frequencies appearing in the first group of the

attached appendix, you will understand that in the sequent letter order of the first strip there is TQW and in the sequent letter order of the first strip of the second group, there is PTW. By comparing the two, you will also understand that the interval T-W of the second group is twice the interval (T-Q, Q-W) of the first group. Therefore, the sequent letter order of the first strip must be P...TQW. By pursuing this comparative study of these two groups, you will get ADTWIVX as the sequent letter order of the fifth strip.

The strip reconstructed through this process may not give the same sequent letter order of the original strip but it serves our purposes.

From the result of the reconstruction of a strip through the study of strips, we derived the following information.

When the interval of each letter of plain and cipher texts of the frequency group, which was the basis of our comparative study, is odd in number, we could call it one and when it is even, we could call it two. However, when it is even, two stripe with interval two could be constructed. A complete strip cannot be made unless these two strips are properly put together. But, if you can discover a third group of the same frequency, you can construct another strip very easily even if the interval of letters of the plain and cipher texts of the frequency group under study is even. It is also clear that the interval of the third group is 13.

It took me about a month to make this study and I have made no further progress. Since it requires a large volume of traffic and number of personnel to perform research on cipher messagee (without any reference to plain text), and since I was not able to concentrate on this study, I designated Mr. ZENKATSU FUJIMI who has previously been performing research on strip ciphers to continue his work.

	1	2	3	4	5	6	7	8	9	10	11	.....(strip numbers)
Group I	T	h	e	j	a	p	a	n	e	s	e	
	Q	S	Y	W	D	A	E	C	.	.	.	
	t	h	r	e	e	p	o	w	e	r	s	
	Q	S	G	R	P	A	X	Q	.	.	.	
	p	r	e	j	u	d	i	c	i	a	l	
	M	N	T	W	C	F	M	W	.	.	.	
	p	r	e	s	i	d	e	n	t	.	.	
	M	N	T	A	V	F	I	C	.	.	.	
	q	u	e	s	t	i	o	n	.	.	.	
	W	D	T	A	W	X	X	C				
	T											
	Q											
	W											

AD, TW, IV

	1	2	3	4	5	6	7	8	9	10	11	12	13	.....(strip numbers)
Group II	T	h	e	j	a	p	a	n	t	i	m	e	s	
	W	M	W	S	T	Z	Q	W	Q	S	XX	N	N	
	p	r	e	l	i	m	i	n	a	r	y			
	T	Q	Y	D	X	.	.	W	.	.	.			
	T	h	a	t	t	h	e	.	.					
	W	M	S	C	I	.	.	.	.					
	T													
	W													
					A	.	.	.	.	.	.	A	D	T	N	I	V	X
					T									
					I									
					X									

The interval of the second group is twice that of the first group. This is clear from the interval in TQW of the first group and the TW of the second group.

	1	2	3	4	5	6	7	8	.	.	.
Group III	n	a	t	i	o	n	a	l			
	Q	U	M	S	S	A	D	C			
	q	u	e	s	t	i	o	n			
	W	A	D	I	M	T	X	F			

V. ASPECTS OF THE RESEARCH SECTION DEALING WITH AMERICAN GOVERNMENT CRYPTOGRAPHIC SYSTEMS

YOSHIKATSU FUJIMI
Specialist, Telegraphic Section
Foreign Office

Beginning on 8 January 1940 this office was presented, first by the Navy, and later by the Army, with copies of various code books in use by the American, British, and other foreign governments. Following are details pertinent to those used by the American Government which were delivered to our office.

January to June (?) 1940:

A. "Gray Code" (in one volume).

B. "Brown Code" (in two volumes, encoding and decoding sections).

C. Only the decoding section of a two-volume code book. The exact designation of this book is not recalled, but the "system" and "volume" are recalled in considerable detail.

D. Two or three types of enciphering tables used for strengthening the security of "Gray Code" text (they differed in dates of use).

E. It is recalled that a number of additional documents were delivered to this office, but the actual articles were destroyed in the fire at this office 7 January 1942, and documents containing results of study by this office were also destroyed as a result of the air raid of 25 May 1945.

The above were all furnished by the Navy.

15 (?) September 1940:

Three copies of a pamphlet, delivered by the Navy, in which was contained part of a "strip cipher" system which the United States boasted as most secure from the point of view of solution, and which they intended to use for their TOP SECRET communications. In this were the following:

A. Alphabet strip:

0-1; 9-1; 10-1; 13-1

B. Daily key table:

0-1; 9-1 (10-1 and 13-1 also used with this)

C. Numerical key:

0-1; 9-1 (10-1 and 13-1 also used with this)

D. In addition, rules for use, indicators, etc. were mentioned.

The first message deciphered through the use of this pamphlet was a message from Secretary of State Hull in Washington to Ambassador Grew in Tokyo, dated 20 Nov 1940. The text was enciphered by means of the "0-1" system, titled "For Intercommunication."

Received from the Army, February and March 1943:

A. Alphabet strip:

4-1; 7-1; 10-3; 33-1

B. Daily key table (identical with 9-1)

C. Numerical key (identical with 9-1)

The following were received from the Army 22 (?) August 1943:

A. Alphabet strip "V"

"V" is a designation given by this office; the actual designation is not known.

B. Daily key; numerical key (identical with 9-1)

Received from the Army August 1944:

A. Alphabet strip (0-5)

B. Daily key, numerical key (0-5)

Received from the Army in February 1945:

A. Alphabet strip:

a. 0-2; 0-3; 0-4 "For Intercommunication"

b. "For Individual Communication" for Chungking, Vladivostok, and several other places

B. Daily keys and numerical keys for use with "A"

VI. DESCRIPTION OF AMERICAN GRAY AND BROWN CODES

Gray Code

This is a 5-letter code, consisting of approximately 150,000 groups of the following characteristics:

First Letter

It is invariably one of the following consonants: B, C, D, F, G, K, L, M, N, P, R, S, or T.

Second Letter

One of the six vowels, including the letter Y.

Third Letter

It is one of consonants M, N, P, R, S, or T when the first letter is one of the consonants B through L. It is, however, one of the consonants, B, C, D, F, G, K, or L when the first letter is one of the following consonants: M, N, P, R, S, or T.

Fourth and Fifth Letters

These are made up of either vowel-consonant or consonant-vowel combinations. Six vowels including the letter Y and 18 consonants excluding the letters F and N are used. The code values are arranged alphabetically, with exception of punctuation marks and other frequently used words such as "a," "the," "quote," "unquote," etc. Proper nouns, syllables, etc., which are not used frequently are invariably assigned to the code groups, the fourth and fifth letters of which are consonant-vowel combinations. In all probability these values of low frequency are arranged in two columns, according to the fourth and fifth letters, in the original code book.

Before we came to the above conclusion, the following processes were followed in the study of this code book:

(1) Sorting of the traffic sent in this code

(2) Frequency studies

(3) Messages were studied against the copies of official documents submitted to the Foreign Office by the American Embassy. Close examination was made of all available material on hand such as cross-system duplicates, etc.

(4) Collation of the results obtained and further study thereof. About the time when the solution of the Gray Code was completed, another code was also solved (our designation for this particular code was "A Code").

The "A Code" is very similar in its appearance to the Gray Code. At a glance the characteristics of the code groups in the "A Code" were almost the same as those of the Gray Code. The code groups were made up of consonant-vowel-consonant-vowel-consonant or consonant-vowel-consonant-consonant-vowel combinations, the consonant which constitutes the first letter being one of either of the following groups of consonants: B, C, D, F, G, H, (K?) or M, N, P, R, S, T, or V. The second letter is one of the six vowels (including the letter Y). If the first letter is one of the consonants B through K, the third is also one of the same group of consonants. If, however, the first letter is one of the consonants M through V, the third letter will be one of that particular group of consonants. It is my recollection that the use of this code book was discontinued in 1933.

Solution of the Cipher Tables Used in Conjunction with the Gray Code:

All messages to and from the American Embassy could be divided into five categories on the basis of the characteristics of the initial group, which appears to be the indicator, and of the code groups themselves. Of the five categories, there were three which appeared to be, on the basis of frecuency characteristics of the code groups, substitution systems. In 1933 we came by chance upon a document which, on the strength of group count, date, etc., we assumed to be the deciphered version of a message

belonging to one of these three categories using cipher tables. On this assumption, we encoded the document by means of the Gray Code of our own reconstruction and the result was studied against the original intercept. It was proved then that our assumption was correct. This gave us a break in the reconstruction of the cipher tables. We were able to reconstruct approximately 20 Gray Code cipher tables within three or four months.

There are two methods of substitution used in conjunction with the Gray Code.

(1) Substitution by two letters, two letters and one letter of each code group.

(2) Substitution by two letters, one letter and two letters of each code group.

It was obvious in the last two categories of systems that the original code books were not being used unenciphered. We abandoned as a hopeless task the study of traffic falling into these two categories as we felt we were not technically equipped to succeed in the solution of complicated systems such as these two.

Brown Code

Beginning in the autumn of 1933 we began to receive traffic which was completely different from previous consonant-vowel combinations as we knew them in the case of the Gray Code and which was not like anything which we had ever encountered previously. As a result of our study of this traffic, it was discovered that it was a 5-letter code, each code group having a 2-letter difference. It was also discovered that no cipher tables were used in conjunction with the new code. We attained fair success in the solution of this code. Although no unusual characteristics of any particular code group from the standpoint of frequency were noted in any single message sent in the new code, when compared with the messages sent in other systems using cipher tables, frequency characteristics of the code groups were rather apparent in the new system.

VII. SOLUTION OF BRITISH FOREIGN OFFICE SYSTEMS

HAYATO KUDOO
Communications Officer
Foreign Office

Within a few months after I joined the Cryptanalytic Section of the Foreign Office in April 1924, study was undertaken of a 5-letter code which was one of the various systems used in traffic to and from the British Embassy. Every member of our section was employed in the solution of this code and as a result in about six months we were able to read up to about 80 percent of the traffic. Apparently this code was in use between the British Government and all its diplomatic representatives abroad. Although the employment of this code was extremely extensive in scope, its use was rather infrequont, making the traffic read in this code rather insignificant as a source of intelligence. Further study of this system,therefore was more or less abandoned and we transferred our efforts to the solution of another 5-letter code. We were also successful in the solution of this code to the extent that within a year we were reading more than 95 percent of the traffic. About three years later this particular code was changed from a 5-letter to a 4-letter system. We were able to read, however, in about seven to eight months after the change was effected, more than 85 percent of the traffic. This code remained in effect for four years. It was then that the code was again changed into another 4-letter code. Some of the code groups were of such combination of letters that it was impossible to pronounce them but this, too, was solved and in about seven months we were reading more than 95 percent of the traffic. There was not a great deal of difference in the method employed in the solution of these systems and the United States diplomatic systems.

Some time during January 1940, a code book and its substitution tables which were in use between the British Foreign Office and its legations abroad were obtained from military sources (I do not recall whether it was

from Army or naval sources). These cryptographic materials made it possible for us to read a great deal of traffic. The substitution tables were changed every four to six months but new tables were always delivered to us from military sources within a month of the date after they went into effect. It was a 4-digit code and the substitution was made on the basis of four groups of five digits each. Each break for substitution was indicated by an indicator. Different indicators were used for each message. Substitutions were made from left to right. It is my recollection that more than six or seven different numerical codes were used by the British Foreign Office.

VIII. MEMORANDUM ON BRITISH GOVERNMENTAL CODES USED AROUND 1940

YOSHIKATSU FUJII
Specialist, Telegraphic Section
Foreign Office

1. Governmental Telegraph Code -

A one-volume book containing about 15×10^4 words.
Each code word was composed of five letters of the alphabet without regard to pronounceability.
The equivalents were arbitrarily arranged.
It was not enciphered.
It was used mainly for commerce, and even after the war broke out it continued in use to some extent as a brevity code.

2. R Code -

A two-volume code (one encoding section and one decoding section).
Each volume contained about 10^4 words.
Each of the code groups was composed of four letters.
The equivalents were arranged arbitrarily.
It was never enciphered and was only used for brevity purposes.
It was in use up until just before the beginning of hostilities but touched on no diplomatic subjects.

3. Inter Cipher -

A two-volume code containing 10^4 words per volume.
Each code word was composed of four digits and the arrangement of the equivalents was arbitrary.
It was used strictly for secret correspondence in connection with a reciphering table.
This strengthened the code materially and the basic groups were never used without recipherment.
The reciphering table was renewed every three months and at the beginning of the lists there was an indicator table (at first only 2000 groups but later 10,000).
After that, there were 100 pages of number lists arranged in random order.
Each page contained 20 lines and each line four groups of five digits.
The indicator consisted of five lines showing which line on which page of the numerical list was to be used, that is, it revealed the starting point.
By its alphabetical order it showed what random additive to take; however, once used, such a number could never be employed again.
At the beginning of the text of telegrams, the message number and the addressee were given in clear, and the indicator was placed directly after them.

Simultaneously with the outbreak of hostilities, this code was ordered stopped.
There also seems to have been a reciphering table for use for individual communication, using the same basic code.
It seems to have been similar to the code just described, but we never broke it.

4. M Cipher -

This was a numerical code similar to the Inter Cipher, and was used from 1935 to the end of 1942.
This, too, had an enciphering table and the indicator showed the date. It was from the date that the starting point was derived; hence, all telegraphs on the same date had the same starting point.
The reciphering table was the same as the Inter Cipher but each page had 15 lines which was five less than the Inter Cipher.
This was used in the main for reports on shipping and the transportation of commodities, never touching on diplomatic matters.
Its use was confined to the commercial attaches of coastal consulates and its use seems to have been limited to the Oriental area.

IX. INTERVIEW WITH MR. OKADA HIROSHI OF THE FOREIGN OFFICE

Mr. OKADA HIROSHI, prior to joining the Cryptanalytic Section of the Foreign Office in October 1944, taught French at the Shizuoka Preparatory School in the Shizuoka Prefecture. In April 1942 French instruction classes were discontinued in all preparatory schools in Japan with the exception of those schools in the Tokyo and Kyoto area. Mr. OKADA taught French at the above-mentioned school from the time of his graduation from the French Literature Department of the Imperial University in 1925. His teaching career covered 19 years.

Mr. OKADA explained that his duties did not entail a knowledge of cryptanalysis. His job with the Cryptanalytic Section was as a translator with the responsibility of improving the readability of translations. He received no formal training of any sort when he joined this particular section. Termination of Mr. OKADA's service with the Cryptanalytic Section came about at the end of the war and at the moment he is attached to the Foreign Office Liaison Office in Osaka.

In the interrogation Mr. OKADA disclosed that there were two French diplomatic systems read by the Japanese. One of these systems was known as 149 and the other CGX. Mr. OKADA does not recall whether they were 3- or 5-letter systems. He asserts that, being a translator, he does not possess any information regarding the technicalities of the cryptographic systems. He had no particular interest in cryptanalytis; his whole interest being occupied in the study of the French language.

These two systems were used in communications between the Foreign Office Embassy in French Indo-China and the French Embassy in Tokyo and possibly in Shanghai. Although these two systems were read up to April or May of 1945, the use of these systems was discontinued as a result of complete occupation of French Indo-China by the Japanese Army which resulted in the suspension of all codes and ciphers by the French in French Indo-China

(the use of these systems was suspended in April or May 1945.)

No French systems were read by the Cryptanalytic Section after April or May 1945. However, a few plain-text messages sent from the French Government quarters in French Indo-China were intercepted. Upon the suspension of use of codes and ciphers by the French in French Indo-China efforts were transferred to the cryptanalysis of Swiss systems. The section succeeded in breaking a 5-digit system used by the Foreign Office in Switzerland and its representatives in Tokyo.

Mr. OKADA recalls that the messages sent in this system had the following characteristics: (1) message always ended with the group "Politique"; (2) the first digit of the first group indicated whether the text was in French or German. If the first digit was odd, the text was in French; when the first digit was even, the text was in German; (3) the code book consisted of encoding and decoding sections.

About May 1945 he was told by his superiors that the study of Swiss diplomatic systems must be undertaken because of receipt from military sources of two copies of the Swiss system mentioned above. The two copies he received were typewritten and complete in every respect. It was apparent that the original code book was compromised but he is unable to give us any information as to where, when, or in what manner the code book was compromised. This system was read by the Cryptanalytic Section up to the termination of the war.

This system was used by the Swiss Legation in Tokyo to transmit to the Foreign Office in Switzerland such information as the general war situation and conditions in Japan.

The French system 149 was used mostly for transmission of such information as personnel matters, wages, etc. The system CGX was used for transmission of far more important information such as the political situation in Japan, the general war situation, etc. The Cryptanalytic Section possessed copies of 149 and CGX. Mr. OKADA does not know when these codes were

compromised because the copies were already there when he joined the section. He heard, however, that these copies were obtained from military sources.

The 5-digit Swiss system mentioned above was apparently made up of two code books, one in French and the other in German. Mr. OKADA does not know whether or not the section was in possession of the code book in the German version. He does not know for sure but he thought all messages transmitted in German were translated by FUKUDA, chief of the Cryptanalytic Section.

He translated an average of two to three messages a day in system 149 and one a day in system CGX. His section received approximately 20 intercepts a day in 149 but they were scanned before they were translated in full. The remainder were put on file, having very little value from the point of view of intelligence. He thought about four to five messages were sent in the 5-digit system of the Swiss Foreign Office, but they were usually long messages and sometimes it took two to three days to complete translation of one important message. As a result, the average was only one message translated in full every two days. All his translations were sent to the Chief of the Telegraphic Department of the Foreign Office. About five or six copies of each translation were made. He had no contact with the Special Intelligence Bureau of the Japanese Army, but he knows that some messages translated by Army translators were being sent to the Foreign Office. Some of these translations were duplicates of the translations that Mr. OKADA turned out, but some were translations of messages which the Foreign Office intercept station failed to intercept. He does not know, however, whether or not these messages were sent in systems other than those being read by the Foreign Office. In most cases the Army was able to translate messages more quickly than his section and he attributed the reason to the far greater number of personnel employed by the Special Intelligence Bureau of the Army.

Mr. OKADA was the sole translator in the French Section. The section consisted of only two persons: Mr. KOIACHI, cryptanalyst, and Mr. OKADA, translator. He states that it was possible that the Cryptanalytic Section had copies of other code books used by the French Foreign Office, but due to the lack of traffic he had no occasion to use any of those code books. The only systems that he recalls having read were, as stated above, 149 and CGX.

X. INTERVIEW WITH MR. KOMACHI SHOOJI

Mr. KOMACHI was born in Toyama-Ken 9 April 1920; he attended Sapporo Dai Ichi High School in 1938 and Tokyo Gaikoku Gakko (Tokyo School of Foreign Studies) from 1941 to 1944. His specialty was French.

In April 1944 he entered the Foreign Office and was assigned as an employee of what he termed the "Black Chamber" (the Japanese title was BUNSHITSU) of the Telegraphic Section. Until August of that year he spent time here making frequency studies, especially of United States systems, and training in general solution problems.

Subsequent to August 1944 he was assigned to the French section, where he was employed in solution activities. The chief of the section at this time was Mr. FUKUDA who had spent five years in the Telegraphic Section, and, besides KOMACHI, there were three other employees, Mr. OKADA, Mr. HAMACHI, and Miss SHIMIZU, all French language specialists.

At the time KOMACHI entered the section, French diplomatic traffic was being read in several systems. Code books of four French systems and one Swiss system were in the possession of the section. These were PC 149, PC 150, PC 151, CGX, and a Swiss system, the name of which was not recalled. All of the French codes had been delivered to the section before he entered.

PC 149, PC 150, and PC 151 were used between the French Foreign Ministry in Paris and its offices abroad in Tokyo, Peking, Hanoi, Nanking, and Chungking. These systems were constituted and used as follows:

PC 149 was a 4-letter system, the first group of which was a 5-digit indicator; KOMACHI does not recall the exact number of indicators assigned each system, but each had a block of numbers for this purpose. The last group in a message was the signature sent in plain text. The second to the last group was composed of five digits, the first three of which ran from 001 to 366 and the last two from 00 to 24, expressing time and date. No substitution tables or additives were used. Although a 4-letter system, messages were sent in 5-letter groups. The system was used for only low-grade traffic

of a personal nature. The code book (decoding section only) was in the possession of the section when KOMACHI entered and he does not know the circumstances of compromise. About five to six messages were read daily up to about March 1945, when the system was discontinued because of a Japanese Army directive prohibiting the use of codes and ciphers in French Indo-China.

PC 150 was also being read at the time KOMACHI entered the section. Its use was discontinued along with PC 149 for the same reasons as above. Only one or two messages were read daily. The first group of a message in this 4-letter system was an indicator of five digits as in PC 149. The last two groups also paralleled PC 149. This code likewise was used for personal matters, and no special efforts were made to read the system as it was of no intelligence value.

PC 151 was a 4-digit code. The first, last, and second to last groups were as above in PC 149 and PC 150. It was sent in groups of five letters, substitution being made on the basis of five groups of four letters each, and decipherment on the basis of a substitution table which converted the letters of the code to digits.

Messages were transmitted in the following manner. The text was arranged in lines of five 4-letter groups, and transmitted in 5-letter groups made by taking successively the first letter of the first groups in the first, second, third lines, etc., followed by the first letters in the second groups of the first, second, third lines, etc., until the requisite 5-letter groups were formed.

XI. DESCRIPTION OF JAPANESE FOREIGN OFFICE WORK ON FRENCH AND SWISS CODES

KOMACHI SHOOJI

I became able to read French codes about August 1944. At that time four French codes were at hand: PC 149, PC 150, PC 151, and PCN 10. I could read them all completely with decoding books. After that, about November 1944, a French code was read by me with the help of KOMIYA and SONODA. In all, five types were used continuously until the Japanese Army took over completely in French Indo-China on 9 March 1945. Then about May 1945 the Army began sending us some Swiss one-part code traffic which we read until 10 August 1945, but the FUKUDA Communications Agency ordered this material burned on 11 or 12 August along with the five French codes (PC 149, 150, 151, PCN 10, CGX). Thus I was familiar with five French codes and a Swiss code, six in all. Now I will describe what I remember.

PC 149 and PC 150

This code has the message number in its caption and also an indicator of five digits. Text follows in groups of 5-letters each and at the end there is a 5-digit group. Three digits give the date and the two last digits give the time. After these digits comes the sender's name. (See Example 1)

Example 1. (PC 149 and PC 150)

```
206 00350 MHCHAM ATNAW IHATW ENASI SIHTE NSUOY NOWET ISNIE MOONO TAHNS
Numoer indicator Il tient plusieurs boutiques à Osaka ;    la plus grande    a
                                              (point virgule)

ITHTS  [illegible]  [illegible]  [illegible]  [illegible]  [illegible] 06009   Cosme
  brule          comme vous  le savez        date time      French Ambassador
     (virgule)                          (point final)
```

Note: Dates, from 001 to 366. Time, from 00 to 24. True also of PC 151 and CGX.

When you decode, the indicator (see Example 3) first shows whether the code is PC 149 or PC 150; once it is determined that it is PC 149 or PC 150, the 5-letter groups following the indicator are divided into 4-letter groups

and they may be read from the code as they stand.

PC 149 pertained to accounts and management, I think, and was limited to business or personal matters in Japan, China, and Indo-China. An average of five or six messages a day appeared.

PC 150 dealt with nothing whatever but personal matters, and was of no practical use to us. As I recall, we got less than one message per day. We wasted little time reading and evaluating this material.

PC 151

This code in point of number, indicator, date, time, and signature is the same as PC 149 and PC 150, but differs in that substitution takes place according to the date group at the end of the message.

The substitution table for this code contains 30 pages, and the date shows which page in the substitution table is to be used. On the proper page of the table the letters are converted to digits. This is done by digraphic substitution, four digits comprising one group. The groups are then read from the 4-digit code. (See Example 2)

Confined to private matters. Of scarcely any importance. Saw no more than four or five messages a month.

Example 2. PC 151

815	01945	OGUDY	TSUMY	RTEML	PTIDO	ATKNO	ADOYO	ULIKI	ITYES	ILOCO
number	indicator	19462	60019	92840	56048	22006	32131	84420	26780	97094

Mais comme elle etait assuree contre l' incendie pour une somme

MEINN	RIBBU	AR.ES	02114		
22231	60504	83496	date	time	COSME
de cent mille yen			21 Jan	1400	

Example 3.

INDICATORS

PC 149	PC 150	PC 151
00000 - 00100	00200 - 00400	00500 - 00800
01000 - 02000	04000 - 06000	07000 - 09000
10000 - 20000	30000 - 40000	50000 - 60000

So, in Example 1, 00350 is PC 150; in Example 2, 01945 is PC 149, as we see. 00123 pertains to neither.

This code was in two volumes: one was the code itself, and the other comprised the alphabets with which to transpose the digits. (Let us call it

a Transposition List.) With these volumes we decrypt. In order to explain more clearly, let us take the following example:

> Dans la deuxième grande guerre plus de 50 millions d'hommes combattaient.

First we convert the message into a digit code, as in Example 4, by use of the code book. (The digits must always be written in lines of 20 each). Next we place above the message the alphabet for the particular day, selected according to the Transposition List (Example 5) and, as in Example 5, we take out the digits which come under each letter in columnar fashion in alphabetical order from A to T. These we assemble in groups of five digits each. The final 4-digit group (2183 in Example 5) is made from random digits in order to complete the line. Then we send the message. If the text of the message had stopped at 2168 instead of 8806 in the third line of Example 4, the following groups (7340,1338,8806) could be simple random numbers, but usually some digit is placed there as a sign.

To decrypt a message like Example 5, we divide it into lines of 20 letters each, omitting the number, date, and time. We then take from the Transposition List the alphabetic key corresponding to the date of the message (in Example 5 019 i.e., 19 January) and, as in Example 4, we write this at the top of the message (as in Example 5). Since there are three lines of 20 letters, this message is composed of three lines of 20 digits (see Example 4).

Example 4. Plain Text No. 205 Jan. 19, 10 P.M.

OIEA	RLHD	MNST	PJFB	QKGC
4544	9608	9197	4670	0909
Lans	la	deuxième	grande	guerre
5165	3020	0229	0323	9212
>	plus	de	50	millions
2168	7840	1338	8806	Name
d'	hommes	combattaient		

Example 5.

205 45803 69280 04667 20010 24511 63892
number

60890 11234 52408 09937 92379 82188

01920 Name.
Date time

We then divide the code message in Example 5 into groups of three in alphabetical order from A to T. But as for the final four letters (in Example 4, QKGC), they divide into groups of two (Example 5). That occure because, if only the last line has 16 digits (four groups) when encodement takes place, the four digits (2188 in Example 5) are random. If the division ends thus, under the first A, we write 458 columnarwise as in Example 4; the same is done with B. Then as in Example 4, when we see the code emerge 4544= dans, 9608=la, 9197=deuxième, etc.

Let us suppose there are ten 20-digit lines in the message in Example 5. In the 20-letter alphabet of the Transposition List those that pertain to the last four letters are divided into nine digits. The other 16 letters are divided into 10 digits and under every letter of that day's alphabet as far as T, in alphabetical order, we write the digits of the code in columnar fashion making 10 lines. Then we decrypt. Naturally each line has 20 digits (five groups) and only line 10 has 16 digits (four groups).

This system deals principally with military situations and we receive about one long message a day in it.

I received messages in the above four codes for about two months from August to September 1944. After 9 November I worked on CGK until March 1945. My memory is therefore not completely reliable.

Example 6.

PCN 10 Transposition Key List

Days of the year from 1 to 366

1	DKOQ	LFJA	THIC	NSMB	EPGR
2	IOQD	KTCL	GNEM	FPBR	ASHJ
3	FLIP	ETJK	BSRA	QGHN	CMOD
4	OCQA	TPFM	BNDS	----	----
5	OSBR	AITQ	----	----	----
6	ETOJ	----	----	----	----
	----	----	----	----	----
19	OIEA	RLHD	MNST	PJFB	QKGC
20					
21					
364	----				
365	-----				
366	----				

N.B. The peculiarity of this List is that the 20-letter alphabet never ran beyond T on any day and ran from 1 Jan to 31 Dec. The letter arrangements all differed. One point to heed when using it was that on page 7 also it is explained that the last four letters are one digit shorter than the other 16, and those corresponding to QKGC in Example 4, are on 1 January EPGR; 2 January ASHJ; 3 June CMOD.

This code's number, as in the case of the other four, is in the preamble. The date and time come at the end, and the indicatore are 5-letter groups. They are the fourth or seventh groups; let us call the former A indicator and the latter B indicator. Both have respective Indicator Lists. Let us call them the A Indicator List and the B Indicator List. These lists have at the same time respective substitution tables which we shall designate Substitution List A (Example 9) and Substitution List B.

Now let us say we receive a message like Example 7. We recognize from the A Indicator List (Example 8) that it has an A indicator. According to Substitution List A (Example 9), we turn the letters into digits which we divide into groups of four digits each. Then according to the code (a code identical with PC 151) the values appear.

Example 7. Code Telegram in CGK

	0	0	0		0
00150	NEIRT	NEMUT	ABSOL	EVAIT	VUOSD
number			A indicator		
IMORT	TAPEM	EMFAN	TRIEN	YERRM	------
	B indicator				
-----	-----	-----	03110	Name	
			Date time		

The text dealt with political matters. We received five or six messages a day. They were of the utmost value.

Example 8. A Indicator List

Indicator	Combination	Page
ABCDE	1245	1
ACOPD	2345	10
BDKLM	1234	5
BPFJX	1345	30
'''''	''''	''
'''''	''''	''
EVAIT	1245	16

N.B. First, in accordance with the indicator combination, we group the message in 20 letters according to Substitution List A (Example 5) and proceed to substitute. In the case of Example 7 the indicator pertains to the A Indicator List and the combination is 1245; the page is 16. Hence in this manner we first convert the digraphs NE, RT, NE, UT, AB, OL, VU, SD, IM, SO into digits, using Substitution Table A. If the combination is 2345, in the case of Example 7, we convert to digits in the following order: EI, RT,

EM, UT, BS, OL, UO, SD, NN, AW; if the combination is 1234, NE, IR, NE, :U, AB, SO, VU, OS, TT, LD; if the combination is 1345; NI, RT, NM, UT, AS, DL, VO, SD, EE, BU. When substitution is completed, decrypt from the code in groups of four letters each. This is like 1062, 5106, 0800, 3512, 4804, in Example 7.

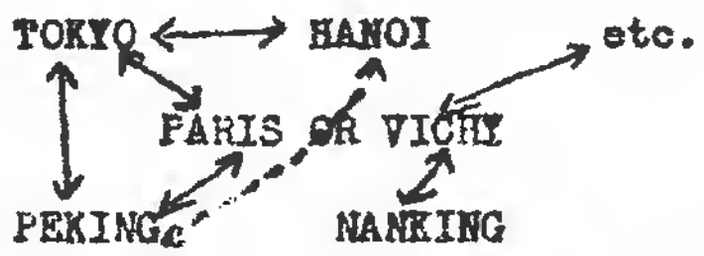
Naturally, in a single message, A and B indicators do not appear. Furthermore, when you substitute, you must be sure to omit the indicator.

Example 9.

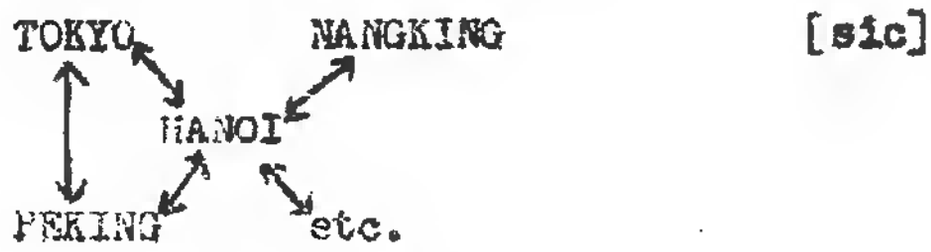
Page 16

AB	00	BA	40	CA	08
AC	20	BC	44	CB	01
AD	18	BD	99	CD	22
AE	82	BE	10	CE	47
AF	28	BF	05	CF	15
-	-	-	-	-	-
-	-	-	-	---	-
-	-	-	-	--	-
-	-	--	-	-	-
-	-	-	-	-	-
-	-	-	-	-	-
-	-	-	-	-	-
-	-	--	-	TA	88
-	-	-	-	TB	27
-	-	-	-	TC	25
-	-	-	-	TD	41
-	-	-	-	TE	80

The above five kinds of French codes were all used in the southern net, as follows:



But when the Anglo-American Forces invaded Normandy in June 1944, the southern net became as follows, as I remember:



Swiss Code

This is a code made up of four items: five pages and 300 groups (Example

10); a substitution table (Example 11); 25 strips of alphabets; and a list (let us call it List S) necessary to show word types, the line of the substitution table, and the number of the strip.

We learned to use these for both sending and receiving.

We determined that, as in Example 10, the code contained 15 pages of eight columns of 25 words each making a total of 200 words per page; thus, 15 pages yielded the total of 3000 words.

The substitution table, as in Example 11, was composed of 15 groups of letters to show the page of the code and eight groups of letters to show the line of the page; that is to say, 23 groups of letters, one line having one group; 100 lines, 100 groups.

There were 25 strips each with a back and front. One surface was called black and the other red. As in Example 12, following the alphabetical order, the first letter of the black and red, as U and L in strip No. 23 of Example 12, was necessarily different; if we follow the order, after Z comes A and between A and Z one letter is displaced. See N in strip No. 23.

Let us suppose we got a code message like Example 14. The message number is 104, and the indicator is the very next 5-letter group, WAPVM. This we substitute according to List S (Example 13).

Since the date is 19 January, according to January in List S, we convert each letter into a digit, making WAPVM become 10623. If the first letter of the indicator gives an odd number (1,3,5,7,9) this code is in French; if an even number (0,2,4,6,8) the language is German.

By the second and third letters we know what line to look for in the conversion chart under Example 11. It is the sixth (these numbers constitute 100 lines; hence they run from 01 to 99 only).

By the fourth and fifth letters we know the number of the strip (Example 12) which we must use. It is No. 23 (these numbers run from 01 to 25 only, because there are 25 strips).

It follows that, this code is in French. We substituted with the sixth

line of the table in Example 11 and we know that the strip was No. 23. Now, depending on whether the number of the strip is odd or even, the substitution order under ATXVB will change. If the strip number is odd, the first two letters (AT) show the page number. Hence, when we observe page AT in the sixth column in the substitution list in Example 11, it is 01; then we use it, and since the third letter shows the letter of the strip we leave it as is. The fifth letter shows the line, in this case a line on page 1. Thus, we observe VB on line 6 of the conversion table (Example11) and make it 8. By means of the substitution order used in case of an odd number on the strip (the fifth letter), we got 10X06. Now, the word that fits this code group coincides with X on strip No. 23, eighth column, page 1. At X, fourth downward in column 8, we find Ambassade. So, 01X06=Ambassade. Proceeding similarly, TWOXM=05006. So the word "France" corresponds 0 on strip No. 23, code page 5, line 6. As a result, we get the result in Example 14.

The strip number does not change even to the end, but if the message is long we insert "passez au rouge" midway and returning backward, employ the red side, but the method is the same. The directions are the same. (The telegram usually begins with black).

As I wrote, if the fifth letter of the indicator, that is, the strip number, is even, the substitution order of the code to follow differs from the case of the odd number; letters one and two show the line; three and four the page; five, as it stands, shows the letter on the strip. Following the substitution table in the example below:

Indicator	1 3 5 7 9	0 0	0	00
		page	letter	line
*	0 2 4 6 8	00	0	00
		line	page	letter

I performed only the substitutions on these messages; I do not know therefore what they contained. OKADA knows quite well what was in them. Six or seven came per day, mostly between Berne and Tokyo. Appended are examples of the Swiss code.

lst Page of the Code

	1	2	3	4	5	6	7	8
1	a,á	abdicataire	aboutir	absolu, e ment		alliance	alterateur trice	amarque tri
2	abaiss, e,r	abdique,r	aboyeur, euse			allié,e,r	altérer	amasse,r
3	abalourdir	abjur,è,e,r	aboyeur, euse				alternatif ve	amateur rice
4	abandon	abime,er						ambassade
5	abandonné e,r	abjur,è,e,r						ambitieux se
6	abat,age							ami,e
23	abattre							amoindrir
24	abbaye	aborder					amadourer	amollir
25	abbe', esse	abonné e	absent,e			alors	amaigrir	amonceler

The length between marque* and amonceler is the identical length of Example 12. That is because this code must conform to the necessary word.

[amarque ?]

Example 11 — Substitution (Conversion) Table

	CODE, PAGE															PAGE, LINE							
1	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	01	02	03	04	05	06	07	08
2	CT	RA	US	CK	LQ	DO	KK	OB	MI	KR	XY	ZA	CO	LY	KI	ZE	LY	CL	NQ	RO	NK	AZ	VS
	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"
5	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"
6	AT	VS	PO	OU	TW	AZ	BA	KN	MK	OR	NQ	CL	LY	ZE	XB	EM	NE	IR	LY	PN	AW	CA	VB
7	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"	"
98																							
99																							
100																							

Example 12.

STRIP

BLACK	RED
No. 23 U	No. 23 L
Y	M
N	O
X	P
Y	Q
Z	R
A	S
B	T
C	U
D	V
E	W
F	X
G	Y
H	Z
I	A
J	B
K	C
L	D
M	E
O	F
P	H
R	I
S	J
T	K

There are 25 such strips. The first letter differs on each. Also on both black and red, as you will see, the first letter differs but the alphabet is regular.
Of course, as there are 25 strips with two surfaces, there are 50 alphabets. There are two strips with the same alphabet, but black does not have an alphabet corresponding to the red in the same order. Also, one letter out of 26 in the alphabet has to be omitted, which, in this example, is N.

Example 13. LIST S

JANVIER	JUILLET
0 1 2 3 4 5 6 7 8 9 A U T N B F C G D O K J M Z E P I H L S V R Y X Q W	
FÉVRIER	AOÛT
0 1 2 3 4 5 6 7 8 9 L H J F E N W T S O D G I U B Z Y M K A C X P Q V R	
MARS	SEPTEMBRE
0 1 2 3 4 5 6 7 8 9 K D N A I L C T B F O P M E H Q G U V R Z W T S X Y	
APRIL	OCTOBRE
MAI	NOVEMBRE
JUIN	DECEMBRE

N.B. From April to Decembre, as in Janvier, Février, and Mars, the alphabet is arranged at will from 0 to 9.

Example 14.

	NAPVM	ATKVB	TWOAW	ATUEM
014	10623	01K08	05006	01U01
number	indicator	ambassade	France	à

NQBIR	ZEYEM	OUTLY	MKFPN
11B03	14Y01	0/T04	09F05
Tokyo	(virgule)	est	fermée

name.

XII. CONCERNING THE TRANSLATION AND SOLUTION OF CHINESE CENTRAL GOVERNMENT ENCODED MESSAGES

DAIZOO YOSHIWARA
Special Employee and Head of Chinese Section,
Annex Room (Special Section) of the Communication Division

History

I engaged in the solution and reading of encoded messages of the Chinese Government by commission of the Foreign Office from 31 January 1940. For many years before I took up this work there had been some solution work done, but as far as is known from the records, practically no progress had been made. It is quite clear now that unnecessary time and money were spent uselessly under the guise that it was for solution research. The message traffic used for solution purposes from that time was received mostly from the Army, Navy, and Communication Departments, and only a few were from the Foreign Office. The code books used for reading, too, were practically all received from the Army and Navy Departments. The number of personnel engaged in this work for the Foreign Office was so weak that it is beyond comparison with the force used by the Army and Navy. This condition continued until the war ended.

Progress Made on Its Solution

From the start, China used the Chinese Character codebook table, which contained about 10,000 characters, as a basis for her encoded messages. Since every character is represented by four digits, by simple manipulation you can encipher the encoded message either by substituting (shuffling) the pages of the Chinese Character table or by re-numbering the vertical and horizontal coordinates on every page of the same.

As explained above, practically all of the code books used by the Chinese Government were received from the Army and the Navy, but as far as the complete solution of "27 DEMPOW" is concerned, it was done after I took up the task.

Future Prospect

Since to date very few encoded Chinese messages use an additive system, one can most likely succeed in reading them if sufficient time is spent in research. However, in the future the Chinese Government, too, may take steps in adopting

additive systems more extensively, in which case its solution will be gradually more difficult.

The Foreign Office has, at present, closed this research so I am not in the position to say what future course will be taken.

XIII. INTERROGATION OF FOREIGN OFFICE PERSONNEL, 9 NOVEMBER 1945

(1) Mr. KONDO:

The above individual was head of the American Section at the time of the fire on 25 May 1945. It was stated, however, that he was not within the compound on this particular evening. Usually it was his custom to leave the office between five or six in the evening, and this particular night proved to be no exception. The following morning he arrived at the Foreign Office grounds to find the debris still smoldering, which prevented him from getting near the building. When queried as to what attempts were made to save valuable equipment and documents, Mr. KONDO admitted he had little knowledge concerning what action was taken in this respect.

It was the conclusion of Mr. KONDO that the American Section, Foreign Office, was completely gutted by the rain of incendiary bombs within the area of the compound, and, therefore, no documents or equipment of value could have been salvaged. In viewing the burned area, he saw no files in the vicinity of this particular building which were in a preserved condition and fit for use. The personnel in this section made no attempt to recover files, records, furniture, or personal belongings; since the fire by that time was uncontrollable and thus prevented them from taking such steps.

Mr. KONDO stated he presumed all classified documents and files had been destroyed and made no further attempts to investigate the matter. As far as he was concerned, in viewing the ruined area, it was impossible to salvage anything, particularly files and records. In this, Mr. KONDO was very insistent.

The American Section of the Foreign Office did attempt to reclaim and restore their files and records by obtaining duplicates from other sections, but the attempt was not a complete success. Of all the sections in the Foreign Office, the code section was the only one with a complete file of records and documents.

Mr. KONDO thought it queer that no record or certification of destruction of these documents was ever officially drawn up, but such was the fact and he admitted-ly was unable to explain the reason. Individuals in higher positions never requested such a certificate of destruction, and thus the entire matter went without

action on the part of those in a responsible position. Of course, he personally believed that such a report should have been drawn up, but again insisted that such was not the case.

Since the newspapers were under strict censorship, they merely reported the destruction of the Foreign Office buildings, making no mention in detail of what had been destroyed in the fire.

On or about 15 August documents having a classification of SECRET or CONFIDENTIAL were destroyed, certain records of a lesser classification being retained. Of the records retained, the information they contained lacked any information of value. It was again established from Mr. KONDO's statemente that all documents were destroyed on or about 15 August, after the Emperor's speech.

Mr. KASE was head of the American Section of the Foreign Office at the time of the destruction of these documents (not Mr. NAKAUCHI). On 20 June Mr. NAKAUCHI was head of the section, but Mr. KASE took over his duties.

A formal circular note was distributed to the various sections to the effect that all documents and records were to be destroyed. This formal circular was instigated by the Foreign Minister, although Mr. KONDO believed the Assistant Minister may have sent this particular note.

The interrogation of Mr. KONDO ended with his suggestion that other individuals more familiar with the details of the fire and destruction of the documents be interviewed.

(2) Mr. OYE:

Following the interrogation of Mr. KONDO, Mr. OYE was introduced to the group. It was brought out in questioning Mr. OYE that the files and records in his particular section were, in the main, current from the end of the war to date. Older files and documents were burned in the big fire of 25 May, and other material was destroyed just before the end of the war.

Information was divulged that files and records of his particular section (code room) were housed in two buildings. One was a two-story wooden building which was also used by the Code Section, while the second was a fireproof building for housing additional files and records. Along with files and records,

certain valuable equipment and supplies were also kept in this fireproof building. All the old files, those not in current use, were moved to another building, which was not destroyed by the fire; but when orders were received of the cessation of hostilities these files were destroyed.

It was repeatedly stated by Mr. OYE that no record was kept of this destruction. The only reason he could advance why no record or certification of destruction was ever made was because instructions had never been received from higher authorities that such a procedure should be instigated.

At the end of July 1945 a conference was held, with the heads of various Foreign Office sections attending, to decide on the destruction of records and files. The Vice Minister sometimes attended these conferences. Due to the bulkiness of the archives and files, it was decided at this time to destroy the files not in current use. Destruction of documents from time to time was on the basis of decisions reached during the conferences. From time to time rulings were promulgated as to what action should be taken in this connection. On about 10 August 1945 a second conference was held and decision to destroy all records and files was reached. (To the best of his knowledge, those attending these conferences were: Chief of the Archives, Vice Minister, and Chief of the Political Section.) Actual burning took place from 10 to 14 August, over a period of three or four days. Mr. OYE gave verbal assurance to the interrogators that everything was destroyed by burning.

A verbal statement was accepted from Mr. KAWAMATA that the documents and files had been destroyed, which was the only proof given of the destruction. Usually a conference was held every Monday, during which matters relating to the handling and destruction of records and files were discussed. There were two buildings which contained records and files, dating back over the past five years. In another building the files dated back from the beginning of the Meiji Era up to 1939 or 1940. Teisha and Showa files were all burned at the end of the war. Constant reference to some of the old files necessitated their retention.

Mr. OYE made no attempt to salvage or save any material or documents from destruction by fire; in his opinion the fire was too fierce and uncontrollable. He claimed that the files in the fireproof building were undamaged, but those in the other buildings were entirely destroyed. They were unable to recover any files from those buildings which had been damaged or burned by the incendiary bombings.

Usually five or six persons were on duty at night in this section, and on this particular evening the situation was normal. The customary working schedule for Mr. OYE's section was on a 24-hour basis, some one being on duty in his section all the time.

At the time of the bombing, fires began raging from three distinct areas and spread throughout the entire compound. On the whole, there was little effort made to prevent the spread of flames, the fire being considered unmanageable. With such a situation presenting itself, Mr. OYE thought it understandable that no records or documents were saved.

(3) MR. NAKAUCHI:

Mr. NAKAUCHI headed the American Section in December 1944. It was brought out that Mr. NAKAUCHI was Consul in Los Angeles during the period prior to and just after the beginning of the war. Information divulged in this interrogation brought out the fact that Mr. KONDO was Mr. NAKAUCHI's assistant in the American Section during his particular tour of duty with this section.

Until 25 May when they were destroyed during the night of the big fire, the files were intact in the American Section. It was not until the morning of the second day after the fire had subsided that Mr. NAKAUCHI arrived in the area to find the buildings still smouldering and everything completely in ruin. After the fire the section was moved to the Treasury Building where operations were resumed. Mr. NAKAUCHI's first inkling of the destruction of the Foreign Office buildings came when a radio announcement was made listing the buildings in the Tokyo area, among these were the Foreign Office buildings.

Mr. NAKAUCHI related that he had been just previously stationed in Bangkok but due to ill health was assigned in the American Section, Foreign Office, to

a job which gave him a chance to recover from his ailing condition.

He stated that he was not too familiar with the status of the files in the American Section, having little or nothing to do with them. He left the American Section in June 1945 and was replaced by Mr. KASE.

To his knowledge, duplicate files of the material in the American Section were not kept, and, therefore, it was impossible to reconstruct the files destroyed during the fire of 25 May.

Mr. NAKAUCHI gave the following facts concerning his personal history:

1932- Attended Clark University, Worcester, Massachusetts, where he studied economics.

1933- Worked in the Japanese Embassy, Washington, D.C.

1934- Resided in Chicago.

1935- Left for Japan and duties with the Foreign Office.

1939- With Foreign Office as representative in Vancouver, British Columbia.

1941- Transferred to Los Angeles where he was Consul.

Mr. NAKAUCHI had little information to advance concerning the American Section.

(4)- Mr. KASE: (Toshikazu / Shunichi)

Information divulged by Mr. KASE showed that he took over the American Section from Mr. NAKAUCHI. He made a distinction in that the American Section, while under his authority, also included the British Section.

The coordination of these two sections was brought about at the specific request of the Foreign Minister. During the time he was head of these sections, there was little activity in relation to American-British activities. About the only thing he inherited was the goodwill of the American-British section, rather than the physical assets.

The particular section he headed was so distributed that he, during his entire term of leadership of this section, never completely became acquainted with his section chiefs and, therefore, had very little knowledge of what was taking place.

It was not his concern what happened to the files and records and this being so he never attended any of the conferences (although it was claimed in a previous interview that he was present at these conferences).

Mr. KASE kept insisting that the Archives Chief had the information we were after. Getting away from the main idea of the interrogation, he stated that the Foreign Office had no indication of pending war with America in November; it began to become apparent in early December. His duties were of such a nature that he had to leave all administrative duties to the section heads and was unable to take care of these details himself.

To the best of his knowledge, no record of certification of destruction was ever drawn up regarding the files and records destroyed during the fire of 25 May or at the end of the war.